UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,860	02/27/2004	William C. Barlow	LOT920040015US1 (046)	7207

46321   7590   04/27/2009
CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER
GUPTA, MUKTESH G

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
04/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/788,860	BARLOW, WILLIAM C.
	Examiner	Art Unit
	Muktesh G. Gupta	2444

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 January 2009*.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4 and 6-17* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-4 and 6-17* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____ .
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____ .
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____ .

DETAILED ACTION

1.   **Claim 5** was cancelled.

Claims 1-4, 6-17 have been examined on merits and are pending in this application.

Response to Arguments

2.   *Claim 1 and its dependent **Claims 4 and 6-7** rejection under, 35 U.S.C. 101, stands as Claims are not amended.*

With due respect to judgment on Examiners ability to analyze for non-statutory subject matter regarding Claim 1, it is still unclear from Claim 1 that, what is being claimed is hardware or software of the Web Conference Provisioning System.

As stated on page 3 of Remarks, Applicant points out that the Claim 1 is directed to a device.

It would have been clear to the examiner, if it would have been precisely stated for analysis of subject matter, "What" the device claimed is in Claim 1.

*a.   Applicant's arguments filed on 01/14/2009 with respect to **Claims 1-4, 6-17** have been considered but are persuasive and in view of the additional clarification of rejection, as stated below.*

b.   Applicants argue that applied Gudjonsson and Nguyen references does not teach in combination Claimed invention and the Examiner's misanalysis

notwithstanding, each of claims 1-4 and 6-7 recite a policy manager having a configuration for processing a policy set forth in a policy document and for processing a request for a Web conferencing from a communicatively linked end user.

c.   Examiner has pointed in preceding paragraph what Gudjonsson explicitly does not teach and what Gudjonsson and Nguyen teach. Gudjonsson does disclose an operator is one who operates or manages at least one cluster. All services and device handlers can access administrative information in the database, e.g., for checking user's accounts and permissions to use the specific service. This allows centralization of service billing policies in the database. Examiner considers Cluster operator as a Manager, which implements various policies for controlling managing and administrating various services, such as Video Conferencing, Web conferencing. Cluster operator is positioned between users and back end services running on various platforms and implements policies through administration tools for managing, controlling and monitoring user accounts, profiles, billing policies, security, authentication and permission for various services as and when user request for services after conforming to the user administration data stored in database, in other words implementing policies from policy document.

Nguyen's from the same field networking art discloses Internet service provider Architecture which provides configuration guidelines in its implementation of providing services on one or more of an operating platform, an

operating environment, and one or more services where resource manager may provide the ability to control and allocate one or more of, resources, services and systems are preferably easier to manage because of the ability to set and enforce policies that control how system resources are utilized, preferably ensuring that customers will receive the assigned service level within a shared resource environment.

The rational to combine these references of Gudjonsson and Nguyen is that they are from the same field of endeavor for providing services to subscribers. Accordingly it would have been obvious to one of ordinary skill in the networking art at the time of the invention to modify Gudjonsson's Cluster Operator using the user management functions (implementing policies), security, and authentication and charging features (billing policies) of the system/network as base for providing Web conferencing services, to incorporate teaching that of Nguyen's from the same field networking art discloses Internet service provider Architecture which provides configuration guidelines in its implementation of providing services on one or more of an operating platform, an operating environment, and one or more services where resource manager may provide the ability to control and allocate one or more of, resources, services and systems are preferably easier to manage because of the ability to set and enforce policies that control how system resources are utilized, preferably ensuring that customers will receive the assigned service level within a shared resource environment.

The motivation would have been for an effective and particular way to utilize resources by virtue of dynamic aggregation and configuration of services and efficiently providing the requested services to the subscribers. All types of service providers can position themselves for growth and agility to handle increasing numbers of subscribers, additional services, and workloads that are more challenging and System architectures of service providers that meet these demands are critical to success.

As regards to Claims 8 and 13, Applicant argues that Gudjonsson fails to disclose "applying at least one policy to establishing criteria to identify a platform for hosting said proposed web conference."

Gudjonsson discloses system and corresponding method of establishing communication session(s) (web conference) between users as a function of their availability and/or communication device(s). By default a cluster 1 will run a basic set of services (establishing criteria for communication session) which offer the following features, allow each user 7 to have a unique identity (criteria) within all clusters, provide each user 7 the ability to connect and be securely authenticated (criteria) by the cluster 1 using that identity, provide each user 7 the ability to define arbitrary sets of data related to that identity, this data is persisted or stored in the database 13, and this data is referred to herein as "presence" data of the user, provide each user 7 the ability to publish a dynamic status information and/or presence information related to their identity (criteria), provide each user 7 the ability to monitor the status/presence of a given set of

other users 7 in the same or different cluster(s), and be notified of any change

thereof; and provide each user 7 the ability to look for other user's identity(is)

using queries by name/group or other useful criteria. For each cluster, there will

be a single scaleable, robust, relational database 13 which contains all of the

data the system uses which must be persistent. The database 13 preferably

contains the profile information kept for each user. The database will also contain

the contact list and blinded list for each user. The contact list is a hierarchy of

groups where a user can be part of more than one group, and a group contains

all of the users it contains and recursively all of the users in groups it contains.

Also stored in the database are the data for the different routing profiles for each

user, along with data which describes which profile is currently active, etc. All

settings for each user's client are also stored in the database. (User information

stored in Database is used to implement and configure user policies by the

Cluster operator using administrative tools).

Basic services which may be provided within each cluster, include

dynamic user properties, contact list and contact notification, that allow users to

subscribe and be notified of the online status of other users, routing service, that

allows users to send requests or invitations for communication sessions (web

conference) to other users, as well as configure how these invitations are

handled depending on the user's current presence information, device

information (PC, PDA, Mobile (different platforms)) and to establish an

communication sessions, as text chat session, voice chat session and web

*conference over networks with other users/service providers. Routing logic (i.e.
which choices are made to decide what to do with a message) may be
implemented, e.g., by an RS 33, in a special-purpose pseudo-programming
language dubbed RoutingTree, which is in essence a tree of nodes where all
non-leaf nodes are decision points and leaf nodes are action nodes. Decisions at
decision nodes can be made on a number of parameters, including the contents
of the message being routed, the time and date, the state of certain parts of the
database, etc. For each user, several different named routing profiles may be
specified. Each routing profile contains a RoutingTree-specified routing logic.
Routing profiles may be defined by the client. One routing profile is always active
as the routing profile to use for incoming messages (which one to use may be
defined by the client), and whenever the client sends a message it specifies
which routing profile to use for the outgoing message. In this way, different
routing profiles may be used for different situations (different device platforms),
i.e. one routing profile for when the user is at work, one routing profile for when
she is at home, one for when the user is on-line, etc. For session initiation (i.e.
inviting another user to a session, accepting an invitation, etc.), in certain
embodiments a subset of the Session Initiation Protocol (SIP, [1]) may be used.
These suffice for users to initiate conferences and invite other users to them or
for two users to initiate a point-to-point conference).*

As regards to Claims 9-11 and 14-17, Examiner thanks Applicant to
pointing out the mistake in citing col. 3, lines 14-27 and lines 28-36 which was a

typo by the examiner.   Corrected col. numbers and line numbers are reflected in rejecting the claims.

As regards to Applicants argument that, "thus no network addresses need to be exchanged between the users", Examiner is citing corrected Col. No.

Gudjonsson discloses as stated in col. 3, lines 14-17, col. 11, lines 35-40, routing service allows users to send invitations to other users to establish an arbitrary communication session (e.g., text chat session, voice chat session, web conference, etc.) over arbitrary networks. As shown in FIG. 7, when the user 7 launches the application, he/she is prompted for his user identity, which includes the address to his operator, and a password to be securely authenticated. At this point, the client 11 connects to the corresponding server 3 and establishes a secure connection with it.

Gudjonsson discloses as stated in col. 11, lines 44-64, col. 13, lines 5-18, if logging on is successful; the ball may open and expose a variety of functions and displays which may be utilized by the user/client. One such function is known as a contact list (e.g., FIG. 8 illustrates a portion of such a list). This list is maintained by the user and may include, e.g., other individuals that the users knows and has contact with and optionally addresses or IDs of the other users. In certain embodiments, the list may show the online status of these other users. This status reflects whether a given user is currently logged in the system or not, thus giving information whether that user 7 is immediately reachable. Actually, users have a range of possible statuses they can specify, e.g., to inform other

users that they are indeed online, but wish to not be disturbed or are temporarily unavailable. The list can easily be organized by defining folders, as well as choose from different display modes. The user can enter new contacts, either by typing in their system/network identity (user ID or UID) (if they know it) or by initiating a search in a directory service, where they can search according to various criteria, such as names, e-mail, et cetera. An exemplary UID assigned to a user is shown in FIG. 12(b). There is no limitation on what kind of invitations can be sent. A sending user 7 is provided with at least a few elementary types of invitations as well as the necessary logic to handle the corresponding communication sessions if they do get established. Referring to FIG. 9, these elementary types include the following: 1) Pages: these consist of short text messages (they are the most simple type of invitations, although they do not imply an acknowledgement from the receiving end; 2) Text Chat: these invitations can establish a real-time text chat session between the users; 3) Voice Chat: these invitations can establish a real-time voice session between the users; and 4) Web Conference: these invitation allow users to share navigation on the Web, such that the Web navigation of one user is reflected on the other user's browser);

Gudjonsson discloses as stated in col. 11, lines 20-30, col. 10, lines 23-46, Referring to FIG. 6, as users 7 have a globally unique identity, connections between users can be forwarded across clusters 1 (i.e., from one cluster 1 to another cluster 1). This may be done via a special service, i.e., the inter-cluster

service that acts as a proxy between services in different clusters. From the point of view of the services involved, the proxy is preferably transparent or substantially transparent. The only limitation is that the cluster operator can configure the inter-cluster service to only allow remote access to a limited set of services. Thus operator specific value added services can be made exclusive for a given cluster. The invitation mechanism does not put any limitations on what type of communication is brokered by a Routing Service (RS). The actual types of communication possible are only limited by the device handlers 10 (and/or client devices 11) available to handle them and another user so desires. The session negotiation does not implicitly involve the exchange of user's network addresses, such as IP number or phone number, in certain embodiments. The benefits of this approach include privacy and the fact that users do not have to worry about how to reach other users. Given an invitation from a user 7, the Routing Service (RS) of the called user 7 (i.e., the callee) will decide how this invitation should be handled, without the calling user 7(i.e., caller) having to know how the communications channel between the users was set-up or on what network. Thus, for example, a voice session might end up in the telephone system without the caller knowing it. It is however up to the actual communication logic invoked whether network addresses actually end up being exchanged, and may be out of the control of the routing protocol and/or the application framework. The decision on whether user anonymity should be maintained for all

communication types is thus up to the operator that operates a cluster in certain

embodiments of this invention.

Therefore, Applicant's arguments are not persuasive regarding all these

features, elements of the present application.

Together Gudjonsson and Nguyen both disclose these features, elements

of the present application hence Examiner respectfully disagrees with Applicant's

arguments on page 2-10.

Applicant has had opportunity to amend the claimed subject matter, and

has failed to modify the claim language to distinguish over the prior art of record

by clarifying or substantially narrowing the claim language. Thus, Applicant

apparently intends that a broad interpretation be given to the claims and the

Examiner has adopted such in the present and previous Office action rejections.

See In re Prater and Wei, 162 USPQ 541 (CCPA 1969), and MPEP 2111.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

3.   **Claims 1-4, 6-17** are rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 6564261 to Gudjonsson et al., (hereinafter "Gudjonsson"),

as applied to **Claims 1-4, 6-17** and further in view of US Patent Application

Publication No. 20030172145 to Nguyen, John V., (herein after "Nguyen*").*

*a.   Regarding **Claims 1-4 and 6-17** Gudjonsson discloses substantially the*

invention as claimed. Gudjonsson does not explicitly disclose "policy manager

having a configuration for processing a policy set forth in a policy document and

for processing a request for a Web conferencing."

b.   Gudjonsson discloses (as stated in col. 7, lines 35-67, col. 8, lines 1-2, col.

11, lines 5-19, col. 34, lines 64-67, col. 35, lines 1-3, col. 34, lines 56-63, A

system/network main function is to provide users with a simple and secure way

of establishing arbitrary communication sessions with other users or services,

running either over IP networks (having Internet Protocol address) or other

networks, e.g., PSTN. It also provides operators (an <u>operator</u> is one who

<u>operates</u> or <u>manages</u> at least one <u>cluster)</u> (as an example, Cluster Operator

controls and manages billing policies) a comprehensive environment in which to

deploy value added services (e.g., search engine services, database services,

shopping services, services for sending users stock information such as stock

prices, <u>video conferencing services</u> which enable user(s) to set up a video

conference via a video conferencing server that is external to the application,

etc.) to their users and to be able to charge for their use, as well as providing

them a way to link their installed base of services over to IP networks. In basic

terms, aspects of the system/network act as a broker(s), and can broker

communication services between two or more people (or their respective

clients/PCs/phones), as well as broker access to value added services, some communications based. Access to the services is provided either by lightweight <u>clients</u>, running on <u>various operating platforms</u> (on their respective clients/PCs/phones) or through <u>gateways</u> for browser based systems, such as WAP (Wireless Application Protocol). The system/network is designed to enable easy building and operation of Value Added Services (VAS), using the <u>user management functions (implementing policies)</u>, security, and authentication and charging features (billing policies) of the system/network as their base. Since the system/network is designed to offer accessibility and mobility, a user will be able to access his or her data and services from virtually any communication device-- computer, mobile phone, handheld devices etc. ensuring a broad reach for Value-Added Services of the system/network. Many services might offer access to chargeable resources, such as the phone system, a cellular telecommunications network, an online shopping network, or the like. This calls for a way to control the access of users 7 to these resources and to away of monitoring their usage. In certain embodiments, the system/network according to this invention may support the notion of <u>account types</u> for users, where each <u>account type</u> gives <u>access</u> to some <u>set of services</u>. In this manner, <u>control </u>of service usage can be <u>administered</u> easily. For more detailed charging, each service can define its own <u>billing policy</u> and act accordingly. Some services might choose to simply log all activity, for later accounting, while others might <u>dynamically monitor</u> the <u>user</u> and their <u>current account situation</u>. One aspect on

the back-end regarding administration is the logging of information. It may be possible to log every detail regarding the operation of the system which might be pertinent to the operator. Which details are logged shall be <u>configurable</u> via an <u>administration tool</u>. It shall be possible to easily import log data from the system into other software packages for analysis and archiving. Back-end administration can be manageable at least through command-line tools or equivalent and optionally through <u>user-interface tools</u>. How <u>registration</u> of users and there <u>accounts</u> is handled may be decided on a <u>per-service basis</u>; in one case it might be through the explicit entering of data and running of administration tools by a service employee, in another it might be through a CGI script or equivalent running the <u>administration tools</u> with <u>data gathered directly from the user</u>.

c.   Gudjonsson does not disclose that policy manager having a configuration for processing a policy, though Gudjonsson does disclose an <u>operator</u> is one who <u>operates</u> or <u>manages</u> at least one <u>cluster</u>. All services and device handlers can access <u>administrative information</u> in the <u>database</u>, e.g., for checking <u>user's accounts</u> and <u>permissions</u> to use the <u>specific service</u>. This allows centralization of service billing in the database. As for servers 3, an exemplary server setup includes a network of servers 3 and one database 13. Such a minimal setup is called a cluster, and represents an <u>administrative structure</u> of the system/network. Each server 3 can be <u>configured</u> to run a certain <u>configuration</u> of services. Each such service is either some integral part of the system/network or some additional service installed by the operator. For example, <u>Web conference</u>

groups have a maximum size of X users which can be set by <u>administrators</u> of

the application. Settings for each component of the back-end are preferably

stored in the DB, from where the component reads them upon startup. These

<u>settings</u> are preferably <u>configurable</u> from the <u>admin tool</u>, which has a connection

to each back-end component and notifies it of <u>changes in settings</u> as is

necessary. FIG. 26 illustrates the admin tool's location in a cluster 1. Adding

users to the application and removing users from it is handled by a separate

admin tool which basically issues a new UID, then writes the user's information

into the database. It shall be possible to run this administration tool from the

command line, for use with CGI programs etc. Examiner views Cluster operator

is positioned between users and back end services running on various platforms

and implements policies through administration tools for managing, controlling

and monitoring user accounts, profiles, billing policies, security, authentication

and permission for various services as and when user request for services after

conforming to the user administration data stored in database, in other words

implementing policies from policy document.

d.   Nguyen does disclose, (as stated in par. 0031, par. 0033, par. 0147, par.

0875-0876, par. 1078-1082, Nguyen discloses system and method for designing,

developing and implementing Internet Service Provider (ISP) architectures.

Establishing an architectural model for the ISP architecture according to the set

of design requirements may include identifying one or more core components of

the architectural model and applying one or more architectural principles to the

architectural model. Core components may include <u>one or more of an operating</u>

<u>platform, an operating environment,</u> and one or more ISP services. The operating

platform may include, but is not limited to, one or more of network equipment,

server systems, and storage equipment. The operating environment may include

an operating system and one or more operating environment tools and

applications. The ISP services may include one or more of basic services, value-

added services, infrastructure services, and <u>operation and management</u>

<u>services.</u> The architectural principles may include, but are not limited to, one or

more of scalability, availability, reliability, manageability, adaptability, security,

performance, and open systems. Questions in the following areas are asked:

general, business-related, support, systems and network management, end-user,

registration, customer care, billing system, service availability, security,

demographic, networking, dialup, directory, email, Web hosting, search engine,

caching proxy, Internet relay chat, FTP, Internet News, and development and

staging. Internet architecture may include a separate zone for security

management features (the multi-level security management zone). Security

management may be defined as the implementation and maintenance of policies,

procedures, and technology to ensure business continuity and protect system

integrity. The depth and breadth of the security management features offered by

Internet architecture may depend at least in part on the application and/or service

and the sensitivity of the systems, data and processes associated with the

application or service, among other factors. Security may pervade all aspects of

architecture, implementation, and administration. Embodiments of the Internet

architecture may also include one or more of, but not limited to: authentication,

authorization, certification, non-repudiation, transaction monitoring, threat

detection, integrity and penetration testing, event logging, and alarm generation.

Internet Service Provider Configuration Guidelines describes policies, guidelines

and principles that may be applied to ISP architectures, as well as services those

ISPs may be expected to deliver and some principles behind the network

architectures that support them. Delivering specific service levels may be

achieved by one or more of, but not limited to, the following mechanisms:

partitioning services, carefully managing server resources, and allocating specific

levels of bandwidth to customers. In service partitioning, services may be

separated according to their logic boundaries, such as Web server, application

server, and database server, and then arranged in a multi-tier configuration on

the available hardware. For example, there are several different types of

application execution platforms including, but not limited to, CGI, JavaScript,

Java servlet, and application server. It may be preferable to separate these

platforms for reasons of performance, security, and feature set. For example, the

CGI execution platform may preferably be separated from other application

servers since this type of Web application presents specific concerns with

respect to security. Therefore, CGI programs are preferably executed on their

own server or a cluster of servers dedicated to this purpose. Controlling

resources within a shared server may be preferable in order to guarantee quality

*of service. In one embodiment, a <u>resource manager</u> may provide the ability to
<u>control and allocate</u> one or more of, <u>resources</u>. Another capability of a resource
manager may be to define hierarchical relationships between resource pools.
Resources may be assigned to a parent pool that includes a number of
subordinate pools, or children. The parent may be assigned resources as usual.
The child pools may be assigned resources from the parent pool. This technique
may be useful, for example, for creating classes of service. The parent
represents the overall class of service and the children represent the individual
customers that belong to the class. Systems are preferably easier to <u>manage</u>
because of the <u>ability to set and enforce policies</u> that <u>control how system
resources are utilized,</u> preferably ensuring that customers will receive the
assigned service level within a shared resource environment. As an ISP moves
into offering Service Level Agreements (SLAs) or meeting higher service levels, it
may be beneficial for the ISP to implement more stringent security policies that
may be required to ensure that subscriber data remains confidential.*

*e.   Accordingly it would have been obvious to one of ordinary skill in the
networking art at the time of the invention to modify Gudjonsson's Cluster
Operator using the user management functions (implementing policies), security,
and authentication and charging features (billing policies) of the system/network
as base for providing Web conferencing services, to that of Nguyen's from the
same field networking art discloses Internet service provider Architecture which
provides configuration guidelines in its implementation of providing services on*

one or more of an operating platform, an operating environment, and one or more services where resource manager may provide the ability to control and allocate one or more of, resources, services and systems are preferably easier to manage because of the ability to set and enforce policies that control how system resources are utilized, preferably ensuring that customers will receive the assigned service level within a shared resource environment.

f.   The motivation would have been for an effective and particular way to utilize resources by virtue of dynamic aggregation and configuration of services and efficiently providing the requested services to the subscribers. All types of service providers can position themselves for growth and agility to handle increasing numbers of subscribers, additional services, and workloads that are more challenging and System architectures of service providers that meet these demands are critical to success.

g.   Therefore, it would have been obvious to combine these two references of Gudjonsson's and Nguyen's disclosures in light of providing a system, method and program to achieve a solution to the above challenges by implementing a well-defined, flexible IT infrastructure that fully integrates Internet technologies with core business systems architectures for providing various services to subscribers.

*Together Gudjonsson and Nguyen disclosed all limitations of **Claims 1-4, 6-17** and hence, are rejected under 35 U.S.C. 103(a).*

As to Claim 1, Gudjonsson teaches system for Web conference provisioning

system comprising a policy manager coupled to at least two different Web conferencing

platforms over a computer communications network (as stated in col. 7, lines 35-60, A

system/network according to certain embodiments of this invention includes a plurality

of client applications and a back-end server system having a plurality of clusters. A

main function is to provide users with a simple and secure way of establishing arbitrary

communication sessions with other users or services, running either over IP networks or

other networks, e.g., PSTN. It also provides <u>operators</u> (an operator is one who <u>operates</u>

<u>or manages</u> at least one <u>cluster</u>) a comprehensive environment in which to deploy value

added services (e.g., search engine services, database services, shopping services,

services for sending users stock information such as stock prices, <u>video conferencing</u>

<u>services</u> which enable user(s) to set up a video conference via a <u>video conferencing</u>

<u>server</u> that is external to the application, etc.) to their users and to be able to charge for

their use, as well as providing them a way to link their installed base of services over to

<u>IP networks</u>. In basic terms, aspects of the system/network act as a <u>broker(s),</u> and can

broker <u>communication services</u> between <u>two or more people</u> (or their respective

clients/PCs/phones), as well as <u>broker</u> access to <u>value added services</u>, some

communications based. Access to the services is provided either by lightweight clients,

running on <u>various operating platforms</u> or through <u>gateways</u> for browser based systems,

such as WAP (Wireless Application Protocol),

said policy manager having a configuration for processing a policy set forth in a

policy document and for processing a request for a Web conferencing from a

communicatively linked end user to select one of said Web conferencing platforms to

host said Web conference (as stated in col. 7, lines 60-67, col. 8, lines 1-67, col. 9,

lines 1-34, col. 23, lines 12-45, col. 9, lines 34-58, col. 11, lines 5-19, col. 34, lines 64-

67, col. 35, lines 1-3, col. 34, lines 56-63, The system/network is designed to enable

easy building and operation of Value Added Services (VAS), using the <u>user</u>

<u>management functions, security, and authentication and charging features (billing</u>

<u>policies)</u> of the system/network as their base. Since the system/network is designed to

offer accessibility and mobility, a user will be able to access his or her data and services

from virtually any communication device--computer, mobile phone, handheld devices

etc. ensuring a broad reach for Value-Added Services of the system/network. FIG. 1

illustrates a plurality of clusters 1 of the system/network which may communicate with

one another, while FIG. 2 illustrates an exemplary cluster 1 of the FIG. 1 embodiment.

Referring to FIG. 2, a basic installation of the system/network includes a number of

interconnected servers 3, each of them running a number of services 5. Such a

collection of servers is called a cluster 1 as shown in FIG. 2. A <u>cluster</u> 1 defines an

<u>address space</u> for services 5, and provides the low-level connectivity for services to

connect to each other, as well as for connections with external servers. Each service

can provide access to its functionality through some well known protocol(s), which are

again built on top of a generic stream model. Thus a <u>service</u> can <u>request</u> <u>another</u>

<u>service</u> by name, and establish a connection with it using a service specific protocol.

Cluster 1 will run a basic set of services. In this basic set of services may offer the

following features: 1) allow each user (or user's client) 7 to have a unique identity within

all clusters; 2) provide each user 7 the ability to connect and be securely authenticated by the cluster 1 using that identity; Referring to FIGS. 3-6, a function of the system/network is to provide the possibility for users 7 to establish arbitrary communication sessions with other users 7. Different types (e.g., voice, video or text) of communication may be established. The system/network handles the initial discovery of the mutual communication channel using "invitations." An invitation is basically a request from one user 7 to another to join him/her in some given type of communication. When a user 7 wishes to establish a communication with another user, he/she will invoke some function within his/her client 11, requesting the client to send an invitation of a given type to some selected user. The user's client 11 will then form the correct SIP message and send it to a special service within the cluster, called the Routing Service (RS). In certain preferred embodiments, each user has a particular routing service provided on the user's user server (US). A function of the RS is to decide what to do with the invitation message. As such, messages are never sent directly between users, but always from a user to another user's Routing Service (RS). The decision logic of the Routing Service is local to the user and thus may be programmed by the user 7 in accordance with the user's desires. Routing logic (i.e. which choices are made to decide what to do with a message) may be implemented, e.g., by an RS 33, in a special-purpose pseudo-programming language dubbed RoutingTree, which is in essence a tree of nodes where all non-leaf nodes are decision points and leaf nodes are action nodes. Decisions at decision nodes can be made on a number of parameters, including the contents of the message being routed, the time and date, the

state of certain parts of the database, etc. For each user, several different named routing profiles may be specified. Each routing profile contains a RoutingTree-specified routing logic. Routing profiles may be defined by the client. One routing profile is always active as the routing profile to use for incoming messages (which one to use may be defined by the client), and whenever the client sends a message it specifies which routing profile to use for the outgoing message. In this way, different routing profiles may be used for different situations, i.e. one routing profile for when the user is at work, one routing profile for when she is at home, one for when the user is on-line, etc. For session initiation (i.e. inviting another user to a session, accepting an invitation, etc.), in certain embodiments a subset of the Session Initiation Protocol (SIP, [1]) may be used. The SIP methods used include, e.g., the INVITE, ACK and CANCEL methods. These suffice for users to initiate conferences and invite other users to them, or for two users to initiate a point-to-point video conference. Whatever the logic is, the Routing Service can end up doing two things: ignore the invitation or forward it to some other service that accepts invitations of the given communication type. Services that accept invitations are called device handlers. Clients 11 are exemplary types of device handlers. All services and device handlers can access administrative information (policy document) in the database, e.g., for checking user's accounts and permissions to use the specific service. This allows centralization of service billing policies in the database. Many services might offer access to chargeable resources; Operator controls and manages the access of users to these resources and to a way of monitoring their usage. The system/network supports the notion of account types for users, where each

account type gives access to some set of services. In this manner, control of service usage can be administered easily. For more detailed charging, each service can define its own billing policy and act accordingly. One aspect on the back-end regarding administration is the logging of information. It may be possible to log every detail regarding the operation of the system which might be pertinent to the Operator. Which details are logged shall be configurable via an administration tool. Back-end administration can be manageable at least through command-line tools or equivalent and optionally through user-interface tools. How registration of users and there accounts is handled may be decided on a per-service basis; in one case it might be through the explicit entering of data and running of administration tools by a service employee, in another it might be through a CGI script or equivalent running the administration tools with data gathered directly from the user).

As to Claim 2, *Gudjonsson teaches system of claim 1, wherein said at least two different Web conferencing platforms comprise a platform selected from the group consisting of a customer premises equipment based platform and a hosted platform* (as stated in col. 7, lines 57-67, col. 8, lines 1-23, col. 23, lines 29-32, col. 28, lines 8-11, col. 7, lines 28-31, col. 17, lines 5-31, col. 32, lines 61-67, col. 33, lines 1-2, col. 32, lines 27-29, lines 34-35, col. 2, lines 51-67, Access to the services is provided either by lightweight clients, running on various operating platforms or through gateways for browser based systems, such as WAP (Wireless Application Protocol). The system/network is designed to enable easy building and operation of Value Added

Services (VAS), using the user management functions, security, authentication and charging features of the system/network as their base. Since the system/network is designed to offer accessibility and mobility, a <u>user</u> will be able to <u>access</u> his or her data and <u>services</u> from virtually any <u>communication device--computer</u>, mobile phone, and handheld devices etc.(customer premises equipment) ensuring a broad reach for Value-Added Services of the system/network. External users 7 and their respective clients 11 (e.g., a user's PC, mobile phone, and/or PDA) can connect to services within the cluster via a special connection service, that typically runs on server(s) (connection servers) at the boundary of the cluster's firewall 9, and listens for connections on a specific port. Different routing profiles may be used for different situations, i.e. one routing profile for when the user is at work, one routing profile for when she is at home, one for when the user is on-line, etc. For every user 7, a certain set of data is stored. The data is kept in key/value pairs call properties. These can be global for everyone to see, private only accessible for the user him self or it can be access controlled. A set of routes where each route is enabled for a user or a group of users as defined in the buddy/contact list. A profile is complete in the sense that for every user there is a route for every mode of communication. User 7 is able to create new profiles, delete profiles, edit profiles etc. and he shall be able to set which profile is currently active. Smart routing is based on the user's currently active profile and basically means that whenever another specific user tries to contact the user using a specific mode of communication that user will be routed to a conversation endpoint or message repository which can handle that mode of communication, based on settings in the profile. Connection Servers lie on the boundary

between the unsecured Internet and the secure Intranet that hosts the cluster 1. Each

CS 21 has two network interfaces, one to the unsecured Internet and one to the secure

intranet. As can be seen, the user servers (US) 19 includes online status service 31,

user routing service(s) (RS) 33, device handlers 35, session service 37, user property

service 39, load balancing service 41, and contact list service 43. Connection servers

(CS) 21 include online status service proxy 51, contact status service 53, and lots of

generic proxies 54. Intra-cluster servers (ICS) 23 include lots of generic proxies 55. The

framework underlying each of these servers includes a UMF 25, notification

broadcasting 57, authentication 59, I/O model 61, protocol compiler 63, and resource

and failure detection 65. Operation and maintenance (O & M) server(s) 64 handles

system configuration (e.g., provision/assignment of users) and/or monitoring of

servers/clients system includes confederated network of server clusters (group) along

with any number of client terminals (customer premises equipment) that connect to the

clusters. Terminals/clients are software entities running under different operating system

platforms or any other device running on some communication network that can have

access to the cluster. Terminals/clients can gain access (selected from the group) to

any number of services running within the cluster, or to services running in other

clusters. The connection between the terminals/clients and the cluster is secure, and

use cryptography).

As to Claim 3, Gudjonsson teaches system of claim 1, further comprising a

firewall disposed between said end user and said policy manager (as stated in col. 8,

lines 18-34, col. 32, lines 30-48, External users 7 and their respective clients 11 a user's

PC, mobile phone, and/or PDA can connect to services within the cluster via a special

connection service, that typically runs on connection servers at the boundary of the

cluster's firewall 9, and listens for connections on a specific port. Streams established

through that service are secure and encrypted. As such, the cluster 1 along with all

connected users 7 and clients 11 can form a virtual private network within which

connections between services can be freely established. Connections can also be

made between services and/or users 7 in different clusters 1, as illustrated in FIG. 1.

Such connections go through a special inter-cluster service, which is also secure and

encrypted. Connection Servers lie on the boundary between the unsecured Internet

and the secure Intranet that hosts the cluster 1. Connection Servers may see all

connected clients' traffic in cleartext, and also contain their own private keys in cleartext.

Because Connection Servers are open to connections from the unsecured Internet and

handle all client communications, they will function as firewalls of sort. Each CS 21 has

two network interfaces, one to the unsecured Internet and one to the secure intranet.

There is no routing performed between the two networks. In certain embodiments,

Connection Servers are able to log every connection and connection attempt. Log

entries include such information as the date and time of day of the connection attempt,

source IP number, user ID used for any authentication attempts and the reason for

authentication failure. For successful connections, Connection Servers additionally log

the time of disconnection and the amount of data transferred in each direction. In certain

embodiments, it is preferred that the Community Operator filters and audits traffic from

the Internet destined for the Connection Servers to prevent hacking and to keep track of

any hacking attempts).

As to Claim 4, Gudjonsson *teaches system of claim 1, further comprising a*

demilitarized zone firewall disposed in between said policy manager and end users

coupled to said policy manager of a public Internet (as stated in col. 32, lines 27-38,

Connection Servers of service providers lie on the boundary between the unsecured

Internet and the secure Intranet that hosts the cluster 1. Connection Servers may see

all connected clients' traffic in clear text, and also contain their own private keys in clear

text. Because Connection Servers are open to connections from the unsecured Internet

and handle all terminals/client (end users) communications, they function as firewalls.

Each CS 21 has two network interfaces, one to the unsecured Internet and one to the

secure intranet. There is no routing performed between the two networks. In certain

embodiments, Connection Servers are able to log every connection and connection

attempt. Log entries include such information as the date and time of day of the

connection attempt, source IP number, user ID used for any authentication attempts

and the reason for authentication failure).

As to Claim 6, Gudjonsson *teaches system of claim 1, wherein said at least one*

policy specifies a platform selection based upon criteria selected from the group

consisting of a number of participants to said Web conference, whether said participants

are internal or external to a private network of said end user, a set of features desired

for use in said Web conference, a security level required for said Web conference, and

a priority of said Web conference (as stated in col. 7, lines 60-67, col. 11, lines 33-64,

col. 12, lines 42-67, col. 13, lines 1-18, col. 33, lines 60-67, col. 34, lines 1-7,

Gudjonsson teaches system/network which is designed to enable easy building and

operation of Value Added Services, using the user management functions, security,

authentication and charging features of the system/network as their base and is

designed to offer accessibility and mobility, a user will be able to access his or her data

and services from virtually any communication device--computer, mobile phone,

handheld devices etc. ensuring a broad reach for Value-Added Services of the

system/network to the user. When the user 7 launches the application, he/she is

prompted for his user identity, which includes the address to his operator, and a

password to be securely authenticated. At this point, the client 11 connects to the

corresponding server 3 and establishes a secure connection with it. If logging on is

successful, the ball opens and exposes variety of functions/services (and further as

stated in col. 7, lines 57-59 , Access to the services (web conference services) is

provided either by lightweight clients, running on various operating platforms or through

gateways for browser based systems) and displays status of on-line/off-line users of the

system, which may be utilized by the user/client. One such function is known as a

contact list. This list is maintained by the user and may include, other individuals that

the users knows and has contact with and optionally addresses or IDs of the other

users. The list can easily be organized by defining folders/groups based on criteria

selected, as well as choose from different display modes. The user can enter new

contacts, either by typing in their system/network identity or by initiating a search in a directory service, where they can search according to various criteria, such as names, e-mail, groups, status, services et cetera. All these services of a cluster 1 may interact with the database 13, which is the repository of all persistent data. This includes both user specific data, service specific data and administrative data. The database can be scaled, made redundant and as robust as the operator wishes, all depending on needs. By selecting users from this contact list, a variety of functions become available to the selecting user 7. To start with, the selecting user 7 can display information about a given contact (e.g., a selected user from the list). There is no limitation on what kind of invitations can be sent. A sending user 7 is provided with at least a few elementary types of invitations as well as the necessary logic to handle the corresponding communication sessions if they do get established. Referring to FIG. 9, these elementary types include the following: 1) Pages: these consist of short text messages (they are the most simple type of invitations, although they do not imply an acknowledgement from the receiving end; 2) Text Chat: these invitations can establish a real-time text chat session between the users; 3) Voice Chat: these invitations can establish a real-time voice session between the users; and 4) Web Conference: these invitation allow users to share navigation on the Web, such that the Web navigation of one user is reflected on the other user's browser. As for web conferencing, this is the name given to the feature of the user 7 being able to join a text conference or a voice conference with all of the other users browsing the same web page as him/her. In web conferences, no user has ownership rights. Web conference groups have a maximum

size of X users (which can be set by administrators of the application). If there are more than this many users viewing the same web page, they will be split into groups of no more than X users. The user interface for web conferences may make it easy for users to create their own text, voice or video conference and to invite users to this conference. It shall also make it easy for the user to see which of the other users in the conference have the capability to join a voice conference or a video conference).

As to Claim 7, *Gudjonsson teaches system of claim 6, wherein said set of features comprises at least one feature selected from the group consisting of screen sharing, slideshow presentations, streaming audio, voice over IP, audio conferencing, the use of on-premise audio equipment, audio recording, joint Web browsing, chat and instant messaging and streaming video* (as stated in col.12, lines 55-67, col.13, lines 1-19, col.24, lines 32-35, col. 25, lines 6-9, By selecting users from this contact list, a variety of functions become available to the selecting user. This information may be a combination of items that the contact has actually defined for him. In addition, a function, which becomes available to the selecting user, is the ability to send invitations to the selected contact/group from the list asking another user/group to join the inviting user in a communication session of a given type (web conferencing). There is no limitation on what kind of invitations can be sent, these elementary types include, Pages, real-time text chat session, real-time voice session and web conference, these invitation allow users to share navigation on the Web, such that the Web navigation of one user is reflected on the other user's browser. FIG. 14 is a flowchart illustrating how

a first user, user #1 can establish a communications session, voice chat, text chat, web

conference, etc., with a second user, user #2 using one or more clusters of the network.

Apart from sending pages, a function of the routing service 33 is to act as a tool with

which users can rendezvous in any kind of session, be it a telephone call, a text chat, a

video conference, or web conference).

As to Claims 8 and 13, Gudjonsson teaches *Web conference provisioning*

method comprising the steps of (as stated in col. 1, lines 12-15, system and

corresponding method of establishing communication session(s) (web conference)

between users as a function of their availability and/or communication device(s)*):*

machine readable storage having stored thereon a computer program for Web

conference provisioning, the computer program comprising a routine set of instructions

which when executed by a machine causes the machine to perform the steps of (as

stated in col. 38, lines 8-32, col. 34, lines 26-49, application (computer program) is

aimed at users who have access to the Internet and an account with an internet service

provider, using computer devices running on various operating systems platforms and

have downloaded/stored/executed their application from the ISP/ Internet. The

system/network is designed to features text and voice capabilities, and is a standard

GUI program with a persistent connection to the server. The "web client" is a very basic

client to the application, which enables users with access to a forms-enabled browser to

send anyone in the community a page and provides users with a simple and secure way

of establishing communication sessions with other users or services, running either over

IP networks or other networks):

establishing criteria for a proposed Web conference (as stated in preceding

paragraphs of claim 1 and col.8, lines 47-65, col.11, lines 44-64, col.28, lines 21-42, by

default a cluster 1 will run a basic set of services (establishing criteria for

communication session) which offer the following features, allow each user 7 to have a

unique identity (criteria) within all clusters, provide each user 7 the ability to connect and

be securely authenticated (criteria) by the cluster 1 using that identity, provide each user

7 the ability to define arbitrary sets of data related to that identity, this data is persisted

or stored in the database 13, and this data is referred to herein as "presence" data of

the user, provide each user 7 the ability to publish a dynamic status information and/or

presence information related to their identity (criteria), provide each user 7 the ability to

monitor the status/presence of a given set of other users 7 in the same or different

cluster(s), and be notified of any change thereof; and provide each user 7 the ability to

look for other user's identity(is) using queries by name/group or other useful criteria. For

each cluster, there will be a single scaleable, robust, relational database 13 which

contains all of the data the system uses which must be persistent. The database 13

preferably contains the profile information kept for each user. The database will also

contain the contact list and blinded list for each user. The contact list is a hierarchy of

groups where a user can be part of more than one group, and a group contains all of

the users it contains and recursively all of the users in groups it contains. Also stored in

the database are the data for the different routing profiles for each user, along with data

which describes which profile is currently active, etc. All settings for each user's client

are also stored in the database);

and, applying at least one policy to said criteria to identify a platform for hosting

said proposed Web conference (as stated in col. 7, lines 35-67, col. 8, lines 1-2 and col.

3, lines 1-17, col. 23, lines 12-45, Basic services which may be provided within each

cluster, include dynamic user properties, contact list and contact notification, that allow

users to subscribe and be notified of the online status of other users, routing service,

that allows users to send requests or invitations for communication sessions (web

conference) to other users, as well as configure how these invitations are handled

depending on the user's current presence information, device information (PC, PDA,

Mobile platforms) and to establish an communication sessions, as text chat session,

voice chat session and web conference over networks with other users/service

providers. Routing logic (i.e. which choices are made to decide what to do with a

message) may be implemented, e.g., by an RS 33, in a special-purpose pseudo-

programming language dubbed RoutingTree, which is in essence a tree of nodes where

all non-leaf nodes are decision points and leaf nodes are action nodes. Decisions at

decision nodes can be made on a number of parameters, including the contents of the

message being routed, the time and date, the state of certain parts of the database, etc.

For each user, several different named routing profiles may be specified. Each routing

profile contains a RoutingTree-specified routing logic. Routing profiles may be defined

by the client. One routing profile is always active as the routing profile to use for

incoming messages (which one to use may be defined by the client), and whenever the

client sends a message it specifies which routing profile to use for the outgoing message. In this way, different routing profiles may be used for different situations, i.e. one routing profile for when the user is at work, one routing profile for when she is at home, one for when the user is on-line, etc. For session initiation (i.e. inviting another user to a session, accepting an invitation, etc.), in certain embodiments a subset of the Session Initiation Protocol (SIP, [1]) may be used. These suffice for users to initiate conferences and invite other users to them, or for two users to initiate a point-to-point conference).

As to Claims 9 and 14, *Gudjonsson teaches method of claims 8 and 13, further comprising the steps of resolving an address to said identified platform* (as stated in col. 3, lines 14-17, col. 11, lines 35-40, routing service allows users to send invitations to other users to establish an arbitrary communication session (e.g., text chat session, voice chat session, web conference, etc.) over arbitrary networks. As shown in FIG. 7, when the user 7 launches the application, he/she is prompted for his user identity, which includes the address to his operator, and a password to be securely authenticated. At this point, the client 11 connects to the corresponding server 3 and establishes a secure connection with it);

imbedding said address in an invitation to participate in said proposed Web conference (as stated in col. 11, lines 44-64, col. 13, lines 5-18, If logging on is successful, the ball may open and expose a variety of functions and displays which may be utilized by the user/client. One such function is known as a contact list (e.g., FIG. 8

illustrates a portion of such a list). This list is maintained by the user and may include,

e.g., other individuals that the users knows and has contact with and optionally

addresses or IDs of the other users. In certain embodiments, the list may show the

online status of these other users. This status reflects whether a given user is currently

logged in the system or not, thus giving information whether that user 7 is immediately

reachable. Actually, users have a range of possible statuses they can specify, e.g., to

inform other users that they are indeed online, but wish to not be disturbed or are

temporarily unavailable. The list can easily be organized by defining folders, as well as

choose from different display modes. The user can enter new contacts, either by typing

in their system/network identity (user ID or UID) (if they know it) or by initiating a search

in a directory service, where they can search according to various criteria, such as

names, e-mail, et cetera. An exemplary UID assigned to a user is shown in FIG. 12(b).

There is no limitation on what kind of invitations can be sent. A sending user 7 is

provided with at least a few elementary types of invitations as well as the necessary

logic to handle the corresponding communication sessions if they do get established.

Referring to FIG. 9, these elementary types include the following: 1) Pages: these

consist of short text messages (they are the most simple type of invitations, although

they do not imply an acknowledgement from the receiving end; 2) Text Chat: these

invitations can establish a real-time text chat session between the users; 3) Voice Chat:

these invitations can establish a real-time voice session between the users; and 4) Web

Conference: these invitation allow users to share navigation on the Web, such that the

Web navigation of one user is reflected on the other user's browser);

and, forwarding said invitation to selected participants in said proposed Web
conference (as stated in col. 11, lines 20-30, col. 10, lines 23-46, Referring to FIG. 6, as
users 7 have a globally unique identity, connections between users can be forwarded
across clusters 1 (i.e., from one cluster 1 to another cluster 1). This may be done via a
special service, i.e., the inter-cluster service that acts as a proxy between services in
different clusters. From the point of view of the services involved, the proxy is preferably
transparent or substantially transparent. The only limitation is that the cluster operator
can configure the inter-cluster service to only allow remote access to a limited set of
services. Thus operator specific value added services can be made exclusive for a
given cluster. The invitation mechanism does not put any limitations on what type of
communication is brokered by a Routing Service (RS). The actual types of
communication possible are only limited by the device handlers 10 (and/or client
devices 11) available to handle them and another user so desires. The session
negotiation does not implicitly involve the exchange of user's network addresses, such
as IP number or phone number, in certain embodiments. The benefits of this approach
include privacy and the fact that users do not have to worry about how to reach other
users. Given an invitation from a user 7, the Routing Service (RS) of the called user 7
(i.e., the callee) will decide how this invitation should be handled, without the calling
user 7(i.e., caller) having to know how the communications channel between the users
was set-up or on what network. Thus, for example, a voice session might end up in the
telephone system without the caller knowing it. It is however up to the actual
communication logic invoked whether network addresses actually end up being

exchanged, and may be out of the control of the routing protocol and/or the application framework. The decision on whether user anonymity should be maintained for all communication types is thus up to the operator that operates a cluster in certain embodiments of this invention).

As to Claims 10 and 15, Gudjonsson teaches method of claims 8 and 13, further comprising the steps of: re-establishing said criteria; and, applying said at least one policy to said re-established criteria to identify a different platform for hosting said proposed Web conference (as stated in col. 8, lines 47-65, col. 15, lines 41-63, In certain embodiments of this invention, by default a cluster 1 will run a basic set of services. In exemplary embodiments, this basic set of services may offer the following features: 1) allow each user (or user's client) 7 to have a unique identity within all clusters; 2) provide each user 7 the ability to connect and be securely authenticated by the cluster 1 using that identity; 3) provide each user 7 the ability to define arbitrary sets of data related to that identity (this data is persisted or stored in the database 13, and this data is referred to herein as "presence" data of the user); 4) provide each user 7 the ability to publish a dynamic status information and/or presence information related to their identity (in a simple case, this status or presence might be whether the user is currently online on his/her PC or not); 5) provide each user 7 the ability to monitor the status/presence of a given set of other users 7 (in the same or different cluster(s)), and be notified of any change thereof; and 6) provide each user 7 the ability to look for other user's identity(ies) using queries by name or other useful criteria. User Server (US)

maintains the user state for a given set of user(s). Keeps track of contact lists and blinded lists for these user(s). Keep track of routing for these user(s). Forwards user status changes to interested CS(s) and ICS(s). Routes pages for these user(s) via routing service RS. UMF User Maps a given local user to mapping function a specific US. Maps a user at another cluster to a specific ICS through the CID associated with the user. Monitor status of various servers in the clusters. Readjusts (re-establishes) maps when a server fails, is removed or added, and notifies other servers as needed. Load balance US(s) and ICS(s). CS Connection Server Listens for connections from clients. Forwards status updates on connected clients to the US(s) that is handling them. Subscribes on status changes from US(s) for the contact lists of connected clients. Forwards the status changes to the clients. Forwards paging from connected clients to user servers US(s) and vice versa).

As to Claims 11 and 16, *Gudjonsson teaches method of claims 8 and 13, further comprising the step of performing said establishing and applying steps responsive to a request to schedule said proposed Web conference* (as stated in col. 24, lines 32-67, col. 25, lines 1-5, FIG. 14 is a flowchart illustrating how a first user (e.g., user #1) can establish a communications session (e.g., voice chat, text chat, etc.) with a second user (e.g., user #2) using one or more clusters of the network. At the first user's request, the first user's client (e.g., PC or phone) forms and sends the INVITE message to the first user's US 19 and to the first user's RS 33 at that US [step 153]. The first user's RS 33 on the first user's US runs its outgoing routing logic and determines what

to do with the message [step 155]. The RS may, for example, ignore the message [step 157], but more likely decides to forward it to the second user's RS 33 at the second user's US 19 (at the same or a different cluster) [step 159]. The second user's RS 33 receives the INVITE message and runs its incoming routing logic as programmed by the second user, to determine what to do with the INVITE message [step 161]. For example, the routing log of the second user's RS 33 may cause the RS to: 1) forward the INVITE message as an SMS message to the second user's mobile phone or some other paging network device like a pager (e.g., if the second user is not currently online) [step 163], 2) forward the INVITE message to the second user's inbox [step 165], 3) forward the INVITE message directly to the second user's currently online client (e.g., PC) [step 167], and/or 4) deliver the INVITE message to another user's RS 33 [step 169].).

As to Claims 12 and 17, *Gudjonsson teaches method of claims 8 and 13, further comprising the step of performing said establishing and applying steps when activating said proposed Web conference* (as stated in col. 13, lines 5-18, col. 33, lines 60-67, col. 34, lines 1-7, col. 23, lines 33-44, col. 27, lines 62-66, col. 28, lines 3-7, There is no limitation on what kind of invitations can be sent. A sending user 7 is provided with at least a few elementary groups or types of invitations as well as the necessary logic to handle the corresponding communication sessions that do get established. Referring to FIG. 9, these elementary types include the following: 1) Pages: these consist of short text messages (they are the most simple type of invitations,

although they do not imply an acknowledgement from the receiving end; 2) Text Chat:

these invitations can establish a real-time text chat session between the users; 3) Voice

Chat: these invitations can establish a real-time voice session between the users; and

4) Web Conference: these invitation allow users to share navigation on the Web, such

that the Web navigation of one user is reflected on the other user's browser. As for web

conferencing, this is the name given to the feature of the user 7 being able to join a text

conference or a voice conference with all of the other users browsing the same web

page as him/her. In web conferences, no user has ownership rights. Web conference

groups have a maximum size of X users (which can be set by administrators of the

application). If there are more than this many users viewing the same web page, they

will be split into groups of no more than X users. The user interface for web conferences

may make it easy for users to create their own text, voice or video conference and to

invite users to this conference. It shall also make it easy for the user to see which of the

other users in the conference have the capability to join a voice conference or a video

conference. For session initiation (i.e. inviting another user to a session, accepting an

invitation, etc.), in certain embodiments a subset of the Session Initiation Protocol (SIP,

[1]) may be used. The SIP methods used include, e.g., the INVITE, ACK and CANCEL

methods. These suffice for users to initiate conferences and invite other users to them,

or for two users to initiate a point-to-point conference. The session service 37 handles

session management. The user that initiates a session (i.e. creates a conference or

initiates file transfer). Other users 7 get invitations to the session, which contain

directions on how to connect to the session. Entry into a session is by invitation only;

and this is preferably handled by the session management server keeping a list of users

that may enter the conference).

Action Final

4.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Muktesh G. Gupta whose telephone number is 571-270-

5011. The examiner can normally be reached on Monday-Friday, 8:00 a.m. -5:00 p.m.,

EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, William C. Vaughn can be reached on 571-272-3922. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MG

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2444